МРНТИ 81.93.29
УДК 004.056.55

https://doi.org/10.51889/2022-2.1728-7901.15

А.А. Зиро [1], Д.Р. Турсумбаев [2], Ж.А. Жайбергенова [3], Ш.Д. Тойбаева [4]*

[1] Әл-Фараби атындағы Қазақ ұлттық университеті, Алматы қ, Қазақстан
[2]Satbayev University, Алматы қ, Қазақстан
[3]Astana IT University, Нұр-Сұлтан қ, Қазақстан
[4]Ғұмарбек Даукеев атындағы Алматы Энергетика және байланыс университеті, Алматы қ, Қазақстан
**e-mail:ziro.aasso@gmail.com*

WHITE BOX ӘДІСІ КӨМЕГІМЕН ЕНГІЗУ ТЕСТІН ӨТКІЗУ

Аңдатпа

Мақалада енуді тексеру әдістері қарастырылады. Ақпараттық жүйенің қолжетімді желілерін оған заңсыз енуден қорғалу деңгейін бағалау мүмкіндігін енгізу тесті деп атаймыз. Тесттің мәні – ақпараттық жүйеге рұқсатсыз кіруге мүдделі киберқылмыскердің көзімен қарау арқылы қауіпсіздік жүйесіндегі кемшіліктерді анықтау. Сценарий бойынша, енгізу сынағын жүргізген кезде, мамандар зерттелетін ақпараттық жүйе туралы бастапқы деректердің басқа көлеміне ие болуы мүмкін – ақпараттық қауіпсіздікті қамтамасыз ету үшін қолданылатын аппараттық және бағдарламалық шешімдер туралы ақпараттың толық болмауынан бастап, оның құрылымы мен ұйымдастырылуы туралы барлық ақпараттың қолжетімсіздігіне дейін. Интернет-ресурсқа зерттеу жүргізілді және ақпараттық қауіпсіздік аудиторының осалдықты жою туралы ұсынысы ұсынылды. SecOps әдістемесі зерттелді, ол ақпараттық қауіпсіздік аудиторына ұйымдағы процестерді автоматтандыру және ондағы осалдықтарды уақытша анықтау арқылы қауіпсіздік мәселелерін шешуге көмектеседі.

Түйін сөздер: аудит, ену тест, ақпараттық қауіпсіздік, SecOPs, IDS, кодты талдау, Kali Linux.

Аннотация

А.А. Зиро [1], Д.Р. Турсумбаев [2], Ж.А. Жайбергенова [3], Ш.Д. Тойбаева [4]
[1]Казахский национальный университет имени аль-Фараби, г. Алматы, Казахстан
[2]Satbayev University, г. Алматы, Казахстан
[3]Astana IT University, г. Нур-Султан, Казахстан
[4]Алматинский университет энергетики и связи имени Гумарбека Даукеева, г. Алматы, Казахстан

ПРОВЕДЕНИЕ ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ С ПОМОЩЬЮ МЕТОДА WHITE BOX

В статье рассматриваются методы тестирования на проникновение. Тест на проникновение является возможностью оценить уровень защиты информационной системы от незаконного проникновения в нее из сетей общего доступа. Суть теста состоит в том, чтобы выявить недостатки системы безопасности, взглянув на нее глазами киберпреступника, который заинтересован в получении несанкционированного доступа в информационную систему. При проведении теста на проникновение, в зависимости от сценария, специалисты могут иметь разное количество исходных данных об изучаемой информационной системе. От полного отсутствия информации об используемых аппаратных и программных решениях, обеспечивающих информационную безопасность, до наличия всех сведений о ее структуре и организации. Проведено исследование интернет-ресурса и предложена рекомендация от аудитора информационной безопасности по устранению уязвимости. Исследована методология SecOps, помогающая аудитору информационной безопасности решить проблемы безопасности за счет автоматизации процессов в организации и свое временному обнаружению уязвимости в ней.

Ключевые слова: аудит, тестирование на проникновение, информационная безопасность, SecOPs, IDS, анализ кода, Kali Linux.

Abstract

CONDUCTING PENETRATION TESTING USING THE WHITE BOX METHOD

Ziro A.[1], Tursumbayev D.[2], Zhaibergenova Zh.[3], Toibayeva Sh.[4]
[1]Al-Farabi Kazakh National University, Almaty, Kazakhstan
[2]Satbayev University, Almaty, Kazakhstan
[3]Astana IT University, Nur-Sultan, Kazakhstan
[4]University of Power Engineering and Telecommunications (AUPET) named after G. Daukeev, Almaty, Kazakhstan

Penetration testing is an opportunity to assess the level of protection of an information system from illegal penetration into it from public networks. The essence of the test is to identify the flaws in the security system by

looking at it through the eyes of a cybercriminal who is interested in gaining unauthorized access to the information system. When conducting a penetration test, depending on the scenario, specialists may have a different amount of initial data about the studied information system. From the complete lack of information about the hardware and software solutions used to ensure information security, to the availability of all information about its structure and organization. The SecOps methodology has been investigated, which helps the information security auditor to solve security problems by automating processes in the organization and his temporary detection of vulnerabilities in it.

Keywords: information Security, audit, penetration testing, SecOPs, IDS, code analysis, Kali Linux.

Кіріспе

Нақты енгізу сынағының мақсаты, шынайы өмірдегі шабуылдағыдай, пайдаланушы мен әкімші тіркелгілеріне, дерекқорларға, құпия ақпаратқа және т.б. рұқсатсыз қол жеткізу болып табылады.

Тестілеу кезінде мамандар зерттелетін жүйенің қауіпсіздік жүйесіндегі осалдықтарды іздеу бойынша барлық әрекеттерді, сондай-ақ белгілі бір шабуылдар жасалған уақытты тіркейді. Бұл деректердің барлығы автоматтандырылған жүйелердің, ақпараттық жүйенің қауіпсіздігін қамтамасыз ететін мамандардың шабуылдарына қарсы әрекет ету тиімділігін талдауға мүмкіндік беретін есепте қамтылған.

Көптеген стандарттар мен әдіснамалардың (OSSTMM, OWASP, BSI, PTES және т.б.), сондай-ақ ену тестілеуін жүргізу құралдарының қолданылуына байланысты аудиторға ең тиімді әдістемелер мен құралдарды тез таңдап, практикада қолдану қиынға соғуы зерттеудің ғылыми-техникалық маңыздылығы болып табылады. Осыған байланысты зияткерлендірілген әдістерді (AI / ML негізінде) және пентестинг құралдарын әзірлеу және зерттеу маңызды ғылыми және практикалық маңызы бар өзекті және уақтылы ғылыми міндет болып табылады.

Pentest концепциясы

Пенетрациялық тестілеу (қысқартылған Pentest) [1] – хакерлік шабуылдарды имитациялау арқылы компьютерлік жүйелердің қауіпсіздігін бағалау әдісі болып табылады. Pentest-тің классикалық тұжырымдамасынан басқа, басқа мақсаттарды көздейтін Red teaming тұжырымдамасы бар [2]. Екі жағдайда да тестілеу әдістемесі аса ерекшеленбейді, енгізу жағдайында мамандар тобы жүйедегі осалдықтардың максималды санын табуға тырысады, содан кейін табылған осалдықтар туралы есеп пен оларды жою бойынша ұсыныстар жасайды. Red teaming жағдайында қызыл команданың жүйедегі барлық осалдықтарды табу міндеті жоқ, олар белгілі бір мақсатты көздейді, мысалы, домен әкімшісін кез келген әдіспен басып алу немесе клиенттік дерекқорға кез келген жолмен қол жеткізу. Классикалық ену сынағы бойынша мамандар орындайтын барлық әрекеттер нақты регламенттерге ие: орындалатын жұмыстардың мерзімдері, жүйемен өзара әрекеттесу деңгейіндегі шектеулер және т.б. Red teaming жағдайында мамандар ешқандай шектеулерге ие емес және нақты ауқымды шабуылды барлық ықтимал құралдарды пайдалана отырып жүргізеді, олар мыналарды қамтиды: физикалық қол жеткізу, әлеуметтік инженерия (бұл классикалық ену сынағы кезінде жиі тыйым салынады) [3].

Ұсынылған шешім

Осы жұмыстың бір бөлігі ретінде веб-қосымшаның енгізу тестілеуін жүргізу әдістемесі сипатталатын болады, ол мыналарды қамтиды: енугізуге тестілеу кезеңдері, қолданылатын бағдарламалық құралдар, сынақ нәтижелері туралы есеп беру және т.б.

№1 кезең – Келісім-шарт жасау және техникалық шарттарды дайындау. Ең алдымен, тестілеу қызметтерін ұсынатын компания мен тапсырыс беруші арасында барлық тестілеуді өткізбес бұрын, келісім мен техникалық тапсырма жасалуы керек. Ол тапсырыс берушінің қажеттіліктерін нақты сипаттауы керек: жұмыс көлемі (сынақтан өткен веб-ресурстар), қолданылатын және тыйым салынған тестілеу әдістері (көбінесе, әлеуметтік инженерия, веб-ресурстың жұмыссыздығы және тапсырыс берушінің ақпараттық жүйесіне физикалық қол жеткізуге тыйым салынады), тестілеу нәтижелеріне есеп беру талаптары, тестілеу әдістемесі, қолданылатын стандарттар және т.б.

№2 кезең – Ақпаратты жинау. Келісімшарт жасалғаннан кейін және барлық қажетті құжаттарды бекіткеннен кейін мамандар енгізу сынағын өздері жүргізетін болады. Енгізу тестілеуін жүргізу кезінде негізгі кезеңдердің бірі ақпарат жинаудың пассивті әдістерін де, сонымен қатар белсенді әдістерін қамтитын мақсат туралы ақпаратты жинау болып табылады:

- қосалқы домендер – егер техникалық тапсырмаға сәйкес домен * .example.kz ретінде көрсетілсе, онда бірінші қадам барлық қолжетімді қосалқы домендерді жинау болып табылады. Негізгі домен

мен ішкі домендер бір серверде орналасуы мүмкін болғандықтан, шабуылдаушы бір доменді бұзып, басқа домендерге қол жеткізуге тырысуы мүмкін. Ішкі домендерді жинау үшін келесі құралдарды пайдалануға болады: theHarvester, knockpy, gobuster, dnsmap және т.б. [4].

- мақсатты сканерлеу – ақпаратты қолмен жинаудан басқа, кейбір осалдықтарды анықтауды қоса, мақсатқа қатысты көптеген ақпаратты жылдам жинауға мүмкіндік беретін көптеген автоматтандырылған тексерулер (сканерлер) бар. Кейбір сканерлер арнайы CMS (wpscan, joomscan, drupwn) үшін бағытталған, кейбіреулері нақты бағдарламалау тілдеріне арналған, кейбір сканерлер үлкенірек және кез келген дерлік жүйені тексереді, мұндай сканердің мысалы Acunetix болып табылады. Ең жиі қолданылатын құрал nmap болып табылады, ол ашық порттар мен ашық порттарда жұмыс істейтін бағдарламалық жасақтама үшін мақсатты сканерлеуге мүмкіндік береді. Nmap сонымен қатар осалдықтарды анықтаумен қоса көптеген автоматтандырылған тексерулерді орындай алатын NSE сценарийлерін қолданады [5].

- каталогтар мен файлдар – веб-қосымшада бар каталогтар мен файлдарды қайталау болып табылады. Көбінесе әкімшілер құрама шабуылдарда пайдаланылатын немесе веб-ресурсты бұзуға тікелей әкелетін маңызды деректерді қамтитын файлдарды немесе каталогтарды жалпыға қолжетімділік үшін қалдыра алады. Бұл файлдар мен қалталарға мыналар жатады: жалпыға ортақ домендегі жүйелік каталогтар мен файлдар, конфигурация файлдары, сақтық көшірмелер, логиндер мен құпия сөздері бар файлдар, әкімшілік функциялар және т.б. Сіз файлдар мен каталогтарды келесі құралдарды пайдалана отырып таба аласыз: feroxbuster, gobuster, dirb, BurpSuite, dirsearch және т.б. Әдетте, мұндай ақпаратты іздеу үшін ғаламтордан табуға болатын үлкен сөздіктер пайдаланылады, бірақ ең тәжірибелі мамандар әртүрлі көздерден, соның ішінде өз тәжірибесінен жинақталған өз сөздіктерін пайдаланады [6].

- ашық көздерден ақпарат жинау. Ашық көздер – мақсат туралы жалпыға ортақ ақпаратты қамтуы мүмкін веб-ресурстар. Бұл көздерге GitHub кіреді [7], ол әзірлеу кезеңінде әкімші ұмытып кеткен веб-бағдарламаның барлық бастапқы кодын қамтуы мүмкін. Мұндай кодта көбінесе деректер қорларынан, FTP серверлерінен және т.б. логиндер мен парольдер болады. Мұндай ақпарат маманға Black Box тестілеуінен White Box тестілеуіне көшуге және осалдықтардың бастапқы кодын тиімдірек талдауға мүмкіндік береді, бұл аса маңызды осалдықтарды табу мүмкіндігін арттырады. Мақсат туралы ақпаратты табудың жалпыға ортақ құралы ретінде Dorks болып табылады [8]. Бұл нақты іздеу сұрауларының жаргон атауы, оның көмегімен Google іздеу жүйесі арқылы неғұрлым мұқият іздеу қамтамасыз етіледі. Жоғарыда аталған құралдардан басқа мақсатты жүйені пайдаланушылардың логин мен құпия сөздері бар тарап кеткен дерекқорлардағы тарап кетулерді автоматты түрде іздей алатын құралдар бар.

3 кезең – осалдықтарды қолмен іздеу. Fuzzing - жоғарыда аталған деректердің барлығын жинағаннан кейін, маман веб-ресурспен тікелей өзара әрекеттесуге кіріседі, бұл табылған ақпараттарды, функционалдылықты зерттеуді және ондағы осалдықтарды fuzzing әдісі арқылы іздеуді білдіреді [6]. Fuzzing - бұл веб-қосымшада аномальды әрекетті тудыруы мүмкін қолданба енгізуіне арнайы жасалған деректерді жіберуді қамтитын веб-қосымшаны тексеру әдісі. Арнайы жасалған пайдалы жүктемелер деректері деп аталады. Қандай пайдалы жүктемелерді беру керектігін маман веб-қосымшаларды сынау тәжірибесін жинақтау процесінде түсіне бастайды, пайдалы жүктемелердің әртүрлі түрлері көптеген факторларға байланысты әртүрлі аномальды мінез-құлық тудыруы мүмкін: веб-ресурс жазылған бағдарламалау тілі, пайдаланылатын дерекқор. , т.б. Мысалы, дерекқор сұрауларының синтаксисінде жалғыз және қос тырнақшалар қолданылады, егер әзірлеуші пайдаланушыдан келетін деректерді сүзу туралы қамқорлық жасамаса, маман тырнақшаны өткізіп, аномальды әрекетті анықтауға тырысады, олар бірге пайдалы жүктеме түрімен маманға SQL инъекциясының мүмкіндігін түсіндіреді [9].

4-кезең – Post эксплуатация және артықшылықтарды кеңейту. Post эксплуатация және артықшылықты ұлғайту - егер сыни осалдық табылса және осал жүйеде қашықтан кодты орындау мүмкіндігі алынса, маман серверде өзінің артықшылықтарын жоғарылату кезеңіне өтеді. Егер ол өзінің артықшылықтарын Әкімшіге немесе түбірлік деңгейге дейін ұлғайта алса, жүйенің толық компромиссі жасалады, артықшылықтардың осы деңгейіне қол жеткізген шабуылдаушы кез келген манипуляцияны дерлік орындай алады [10].

5-кезең – Есеп беру. Енгізу тестілеуінен кейін маман табылған осалдықтар туралы есеп жасайды, онда мыналар болуы керек: табылған осалдықтардың әрқайсысын пайдалану кезеңінің толық сипаттамасы, табылған осалдықтардың әрқайсысын жою бойынша толық ұсынымдар, градация. Есеп

беруде OWASP Top 10 немесе сипаттамасы бар басқа әдістеме бойынша осалдықтар, сенімді көздерден осалдықтың сипаттамасы және оны жою бойынша ұсыныстары бар қосымша материалдарға сілтемелер, маман орындаған әрекеттердің сипаттамасы және пайдаланылатын құралдардың атауы, егер олар шабуылға жол бермесе, маман тап болған қорғаныс құралдары туралы ақпарат жазылады [11].

Енгізу тестілеуінен кейін аудитор іске кіріседі, оның мақсаты - енуді тексеру нәтижелері бойынша компанияның ішкі процестеріндегі әлсіз жақтарды қоса алғанда, барлық сәйкессіздіктерді анықтау болып табылады. Мұндай мысал ретінде енуді тестілеу кезінде табылған сыни SQL инъекциялық осалдықты келтіруге болады, аудитор үшін осалдықтың осы түрінің болуы веб-ресурсты әзірлеушілер арасында ақпараттық қауіпсіздік саласындағы құзыреттіліктің жоқтығын көрсетеді. Компанияның барлық қызметкерлері жүйелі түрде ақпараттық қауіпсіздік бойынша хабардар болу курстарынан, біліктілікті арттыру курстарынан, кибергигиена курстарынан және т.б. өтуі керек. Әзірлеушілер әртүрлі салаларда, соның ішінде ақпараттық қауіпсіздікті қоса алғанда, кәсіби даму курстарынан өтуі керек, бұл әзірлеушілердің біліктілігін, олардың хабардарлығын арттырады және осал веб-қосымшалар кодын жазу мүмкіндігін азайтады. Дегенмен, бұл осалдықтың пайда болуы бірқатар жұмыс істемейтін процестерді көрсетуі мүмкін: веб-серверді конфигурациялау процедурасы зардап шегеді, орнатылған брандмауэр дұрыс конфигурацияланбаған, осыған байланысты тестілеу кезінде пайдалы жүктеме байқалмайды, SIEM жүйесі дұрыс жұмыс істемейді, бұл көрінбейтін шабуылға әкеледі және т.б. [12].

Нәтижесінде аудитор тек сынақ нәтижелері туралы есепке сүйене отырып, ұйымның ішкі процестеріндегі көптеген сәйкессіздіктерді анықтай алады.

Келесі қадам тестілеу кезінде табылған осалдық туралы есеп негізінде шағын мысалды қарастыру болып табылады. White Box әдісін қолдану арқылы тестілеу нәтижесінде веб-ресурстың әкімшілік тіркелгісін ұрлауға мүмкіндік беретін жоғары деңгейдегі осалдық анықталды:

Қауіпсіз нысанды десериализациялау + Type Juggling арқылы есептік жазбаны ұрлау

OWASP Top 10 рейтингі бойынша: A2:2017 - бұзылған аутентификация

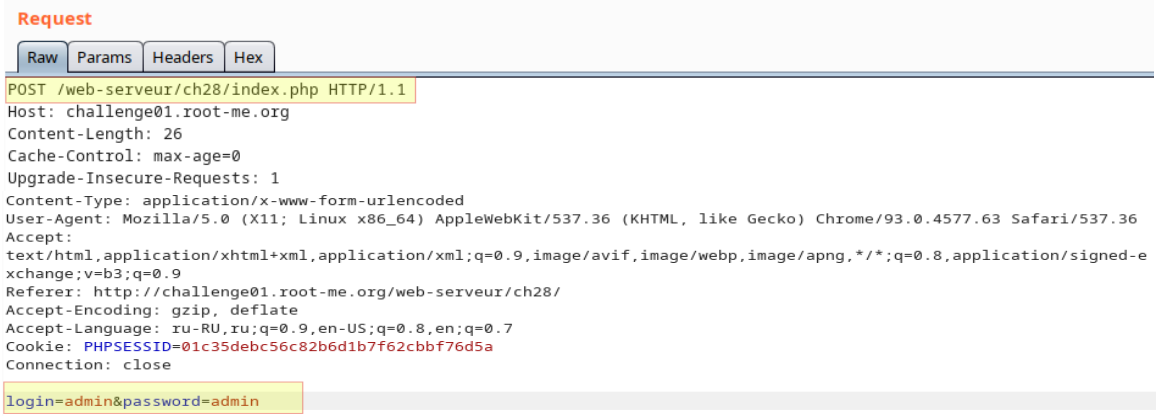
Ауырлығы: жоғары

Бастапқы осал код: /web-serveur/ch28/index.php

Осал жолдар: 15-30

Сипаттама: http://challenge01.root-me.org/web-serveur/ch28/ жолында веб-ресурстың басқару панелінде авторизация пішіні табылды; бастапқы кодты талдау кезінде көптеген осалдықтар анықталды, олар шабуылдаушыға веб-ресурстың әкімші тіркелгісін басып алуға рұқсат бере алады. 1-суретте авторизация нысаны, 2-суретте авторизация сұрауы көрсетілген.

Сурет 1. Рұқсат беру нысаны



Сурет 2. Авторизация сұранысы

Осалдықты жаңғырту 3 суретте корсетілген:

```
/******** AUTHENTICATION *******/
// login / passwords in a PHP array (sha256 for passwords) !
require_once('./passwd.inc.php');


15  if(!isset($_SESSION['login']) || !$_SESSION['login']) {
16      $_SESSION['login'] = "";
17      // form posted ?
18      if($_POST['login'] && $_POST['password']){
19          $data['login'] = $_POST['login'];
20          $data['password'] = hash('sha256', $_POST['password']);
21      }
22      // autologin cookie ?
23      else if($_COOKIE['autologin']){
24          $data = unserialize($_COOKIE['autologin']);
25          $autologin = "autologin";
26      }
27
28      // check password !
29      if ($data['password'] == $auth[ $data['login'] ] ) {
30          $_SESSION['login'] = $data['login'];
```

Сурет 3. Бастапқы осал код

1. Сәтсіз авторизация әрекетінің нәтижесінде суперәкімші пайдаланушысының хабарламасы көрсетіледі, ол жүйеде жоғары артықшылықтарға ие superadmin атты пайдаланушы бар екенін көрсетеді.

2. Пайдаланушыны авторизациялау кезінде код деңгейінде логин мен пароль параметрлерінің POST арқылы берілуі тексеріледі. Параметрлерді пайдаланушы жіберген болса, осалдықты жүзеге асыру мүмкін емес.

18 жол

Код: if ($ _ POST ['логин'] && $ _POST ['пароль']) {……}

3. Егер логин мен пароль параметрлері өткізілмесе, автологин параметрі COOKIE файлына жіберілді ме, басқа шарт тексеріледі. Бұл шарттың денесі COOKIE файлында автологин параметріне жіберілген нысанды қауіпті сериядан шығаруды орындайды.

23 жол

Код: if ($ _ COOKIE ['autologin']) {……}

4. Осалдықты іске асыру үшін кейінірек сериядан шығару функцияларына енетін сұраудағы COOKIE автологин параметрін ғана беру қажет. Автологин параметрі сүзгіден өтпегендіктен, шабуылдаушы өзінің серияланған нысанын өткізе алады, осылайша деректер массивінің мәндерін және оның логин мен құпия сөз мәндерін өзгертеді.

24 жол

Код: $ деректер = сериядан шығару ($ _ COOKIE ['autologin']);

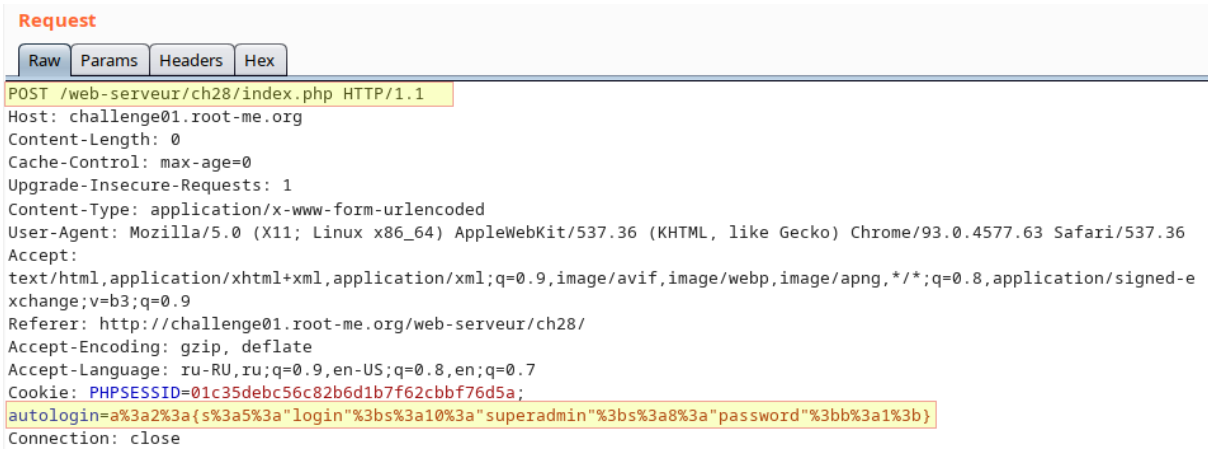
5. Деректер массивінің логин мен пароль мәндерін шабуылдаушы қауіпті сериядан шығару арқылы өзгерткеннен кейін, бұл мәндер айнымалылар арасында типсіз салыстыруды білдіретін Type Juggling осалдығын қамтитын салыстыру функциясына беріледі. Айнымалылар арасындағы салыстыру қауіпсіз салыстыру операторы емес екі тең (==) пайдаланылады.

29 жол

Код: if ($ деректер ['пароль'] == $ аутентификация [$ деректер ['логин']]) {… ..}

6. Әртүрлі пайдалы жүктерді тасымалдау нәтижесінде, егер сіз біреуге (1) тең құпия сөзді өткізсеңіз, онда бір және хэширленген пароль мәнін типтелмеген салыстыру арқылы, салыстыру нәтижесі True және шабуылдаушы болатыны анықталды. логин пайдаланушының құпия сөзін білмей ауысқан пайдаланушының астында авторизациялай алады, бұл жағдайда superadmin, 4-сурет.

Пайдалы жүктеме: a: 2: {s: 5: "логин"; s: 10: "superadmin"; s: 8: "password"; b: 1;}, 5-сурет.



Сурет 4. Пайдалы жүктемесі бар авторизация сұрауы

Сурет 5. Superadmin атымен авторизация

Осалдықты жою бойынша ұсыныстар

1. Бұл жағдайда автологин параметрінде COOKIE сериясын жою үшін пайдаланылатын код артық болып табылады және пайдаланушыны авторизациялау процесіне қатыспайды, егер ол пайдаланылмаса, бұл кодты жою ұсынылады.

2. Егер жоғарыда аталған код пайдаланылса, пайдаланушыдан келетін параметрлерді сүзуді, соның ішінде серияланған нысандарды іске асырудан сүзуді жүзеге асыру ұсынылады.

3. Түзету режимін өшіріңіз.

4. Type Juggling осалдығын жою үшін терілген мәнді салыстыруды пайдалану ұсынылады, яғни. екі (==) орнына үш бірдей (===). Үш тең мәнді пайдаланған кезде, салыстырылатын айнымалылардың мәндерінен басқа, салыстырылатын айнымалылардың деректер түрі де тексеріледі.

Осы осалдық туралы есепке сәйкес аудитор компанияның ішкі процестеріндегі көптеген сәйкессіздіктерді анықтай алады:

1. Осы қосымшаны әзірлеушілер әкімшілік аймаққа рұқсат беру панелін әзірлеу кезінде көптеген өрескел қателіктер жіберді, бұл олардың құзыретінің жоқтығын және, ең алдымен, ақпараттық қауіпсіздік саласындағы әзірлеушілердің біліктілігін арттыру бойынша тұрақты курстардың жоқтығын көрсетеді [13].

2. Ұйымда бастапқы кодты автоматты сканерлеу құралдары жоқ, бұл қорытынды тестілеу кезінде табылған осалдықтардың танымалдығы туралы ақпаратқа негізделуі мүмкін, барлық заманауи бастапқы код сканерлері мұндай осалдықтарды анықтауға қабілетті.

3. Брандмауэрдің болмауы немесе дұрыс конфигурацияланбауы, бұл жағдайда тасымалданған пайдалы жүктеме байқалмады және осалдықты пайдалану сатысында тоқтатылды.

Бұл мысалда көрсетілгендей, енуге тестілеуден кейінгі аудиттің тиімділігі сынақ нәтижелері бойынша бірқатар сәйкессіздіктерді анықтауға қабілетті жеткілікті тиімді шара болып табылады.

Бүгінгі таңда көптеген компаниялар SecOps әдістемесін енгізуде [14], ол ақпаратты қорғау процесіне автоматтандыруды енгізуді білдіреді. EMA есебіне сәйкес, бұл әдістемені көбінесе бағдарламалық жасақтаманы әзірлеушілер, банктік және қаржылық ұйымдар, көтерме жеткізушілер, өндірістік кәсіпорындар және т.б. Әдетте, осы әдістемені енгізген компаниялар келесі көрсеткіштерді арттырады: деректер сапасы, ақпарат қауіпсіздігі туралы хабардар болу, пайдаланушылардың өзара әрекеттесуі жақсарды және ұйым ішіндегі ең тиімді процестерді жылдам анықтауға кірісті. Әдістеменің өз міндеттеріне мыналар кіреді: ұйымның қауіпсіздік деңгейін арттыру, ұйымды басқаруды жақсарту үшін командаларды біріктіру, ақпараттық қауіпсіздік және оның бизнес-процестерге қалай әсер ететіндігі туралы хабардар болу, сенімді құралдарды енгізу арқылы процестерді автоматтандыру [15].

SecOps әдістемесін енгізу процесі бірнеше кезеңнен өтеді: тәуекел аудиті, тәуекелді бағалау, ұйымдағы кибергигиеналық тексеру, бизнес-процестермен интеграция. Енгізу тестілеуінен кейін аудитор көптеген жұмыс істемейтін немесе жеткіліксіз жұмыс істейтін процестерді анықтай алатындықтан, SecOps әдіснамасын енгізу кезінде бұрын сипатталған процестерді реттеуге болады, ал кейбіреулерін автоматтандыруға болады. Мысалы, бұрын аудитордың мысалын қолдана отырып, ену тестісінің нәтижелері бойынша аудитор ұйымда бастапқы кодты автоматты түрде сканерлеуге арналған құралдардың жетіспеушілігін анықтады, бұл әзірлеушілер тарапынан анықталмаған қателердің пайда болуына және шабуылдаушы тарапынан осалдықтарды пайдалану мүмкіндігі. Бұл жағдайда әдістеменің мақсаты осалдықтарды табу үшін бастапқы кодты және қауіпсіздік сканерлерін талдаудың автоматтандырылған құралдарын енгізу болып табылады [16, 17]. Жоғарыда аталған автоматтандыруға қосымша, SecOps әдістемесі ұйымға пайдалы келесі құралдарды енгізуді білдіреді:

- бақылау тақталары – мәселені тезірек табу үшін жиналған ақпаратты жинау және визуализациялау;
- автоматтандыру – жиналған мәліметтерді автономды өңдеу және табылған қателерді жою үшін алгоритмдерді іске қосу (мысалы, дискілік кеңістікті босату үшін журналдарды тазалау);
- қателерді іздеу – қателерді автоматты түрде іздеу және анықтау құралдары;
- ортақ пайдалану - енгізілген жаңа технологиялар бойынша құжаттаманы жариялау;
- визуализация – мәліметтерді талдау және қарау құралдары;
- шабуылды модельдеу – шабуылдарды жіктеу және шабуылдар арасындағы байланыстарды сипаттайтын және ықтимал шешімдерді ұсынатын ортақ үлгіні құрастыру;
- және т.б.

Қорытынды

Зерттеу нәтижесінде барлық кезеңдер сипатталған: ену тестілеуі және ақпараттық қауіпсіздік аудиті. Болашақта нейрондық желі мен AI көмегімен автоматтандыруға болатын осалдық көрсетілді. SecOps әдіснамасын енгізу ұйымның ақпараттық қауіпсіздігінің күрт артуына әкелуі керек. Бұл тәсіл ұйымның көптеген әлсіз жақтарын анықтауға мүмкіндік береді, содан кейін ақпараттық қауіпсіздік деңгейін жақсарту, ішкі процестерді құру және оларды автоматтандыру үшін қажетті шараларды қабылдайды. Барлық қажетті кезеңдерден өткеннен кейін, біз қазіргі уақытта қорғаудың жоғары деңгейіне ғана емес, сонымен қатар қауіптерді ерте анықтауға және автоматтандырылған, жұмыс істейтін ішкі процестерге қажетті барлық құралдарға ие ұйымды аламыз. Әрі қарайғы зерттеулерде параметрлер моделін және нейрондық желі моделін жасау жоспарлануда, оның негізінде IP-ды ену үшін тестілеудің интеллектуалды әдісін құру жоспарлануда.

Пайдаланылған әдебиеттер тізімі:

1 Gnatyuk S Critical Aviation Information Systems Cybersecurity? NATO Science for Peace and Security IOS Press Ebooks, 2016. Vol.47. – №3. – P. 308-316.

2 National Institute of Standards and Technology Special Publication 800-115 Natl. Inst. Stand. Technol. Spec. Publ. 800-115, 80 pages (Sep. 2008)

3 Goel S., Chen V. «Information security risk assessment – a matrix-based approach». University at Albany, SUNY. 2005.

4 Imran, M. S., &Mondal, S. A. (2013). The effect of marketing audit to enhance company performance and marketing accountability. Retrieved from http://www.wbiconpro.com/523-Imran.pdf. 73 Kamil VANA, L. C. (2014). The Marketing Audit as a Method of the Evaluation of the Marketing Plan. 132.

5 Kotler, P. (2002). Marketing Management, Chapter3: Winning Markets Through Strategic Planning, Implementation, and Control (Eleventh ed.). New Jersey, USA: Pearson Custom Publishing.

6 Kotler, P.; Keller, K.L. (2009) Marketing. Management, 13th edition, Pearson International Edition

7 Повышение привилегий и POST эксплуатация в Windows. Блог крупной организации занимающейся информационной безопасностью. URL: https://securixy.kz/own-research/povyshenie-privilegij-v-windows.html/ (Дата обращения 22.03.2022)

8 Блог крупной Российской компании Positive Technologies, Повышение привилегий URL: https://www.securitylab.ru/news/tags/повышение+привилегий/ (Дата обращения 22.03.2022)

9 Крупнейший ресурс для IT профессионалов, Отчет по пентесту: руководство и шаблон. URL: https://habr.com/ru/company/npoechelon/blog/337824/ (Дата обращения 22.03.2022)

10 Фленов М. Е. Web-сервер глазами хакера, 3-е издание, переработано и дополнено – СПб.: БХВ-Петербург, 2021.

11 Блог организации IT GUILD, Как SecOps превращается в инструмент поддержки любых бизнес-операций. https://it-guild.com/info/blog/kak-secops-prevrashhaetsya-v-instrument-podderzhki-lyubyh-biznes-operaczij/ (Дата обращения 22.03.2022)

12 Aitkhozhayeva Y.Zh., Ziro A. A., Zhaibergenova Zh. A., Baltabay A.G. Penetration testing. Bulletin of National Academy of Sciences of the Republic of Kazakhstan, №6 (376).- Алматы: Наука, 2018. - с. 39-44. ISSN: 1991-349421. DOI: 10.32014/2018.2518-1467.25. (Scopus, Web of Science, IF 0.094 по КазБЦ).

13 Gnatyuk S. Critical Aviation Information Systems Cybersecurity? NATO Science for Peace and Security IOS Press Ebooks, 2016. Vol.47. – №3. – P. 308-316.

14 National Institute of Standards and Technology Special Publication 800-115 Natl. Inst. Stand. Technol. Spec. Publ. 800-115, 80 pages (Sep. 2008)

15 Goel S., Chen V. «Information security risk assessment – a matrix-based approach». University at Albany, SUNY. 2005.

16 Imran, M. S., &Mondal, S. A. (2013). The effect of marketing audit to enhance company performance and marketing accountability. Retrieved from http://www.wbiconpro.com/523-Imran.pdf. 73 Kamil VANA, L. C. (2014). The Marketing Audit as a Method of the Evaluation of the Marketing Plan. 132.

17 Kotler, P. (2002). Marketing Management, Chapter3: Winning Markets Through Strategic Planning, Implementation, and Control (Eleventh ed.). New Jersey, USA: Pearson Custom Publishing.

References:

1 Gnatyuk S. Critical Aviation Information Systems Cybersecurity? NATO Science for Peace and Security IOS Press Ebooks, 2016. Vol.47. – №3. – P. 308-316.

2 National Institute of Standards and Technology Special Publication 800-115 Natl. Inst. Stand. Technol. Spec. Publ. 800-115, 80 pages (Sep. 2008)

3 Goel S., Chen V. «Information security risk assessment – a matrix-based approach». University at Albany, SUNY. 2005.

4 Imran, M. S., &Mondal, S. A. (2013). The effect of marketing audit to enhance company performance and marketing accountability. Retrieved from http://www.wbiconpro.com/523-Imran.pdf. 73 Kamil VANA, L. C. (2014). The Marketing Audit as a Method of the Evaluation of the Marketing Plan. 132.

5 Kotler, P. (2002). Marketing Management, Chapter3: Winning Markets Through Strategic Planning, Implementation, and Control (Eleventh ed.). New Jersey, USA: Pearson Custom Publishing.

6 Kotler, P.; Keller, K.L. (2009) Marketing. Management, 13th edition, Pearson International Edition

7 Povysheniye privilegiy i ekspluatatsiya POST v Windows. Blog krupnoy organizatsii, zanimayushcheysya informatsionnoy bezopasnost'yu. URL: https://securixy.kz/own-research/povyshenie-privilegij-v-windows.html/ (Data obrashcheniya 22.03.2022)

8 Blog krupnoy Rossiyskoy kompanii Positive Technologies, Povysheniye privilegiy URL: https://www.securitylab.ru/news/tags/povysheniye+privilegiy/ (Data obrashcheniya 22.03.2022)

9 Krupneyshiy resurs dlya IT-professionalov, Otchet po pentestu: rukovodstvo i shablon. URL: https://habr.com/ru/company/npoechelon/blog/337824/ (Data obrashcheniya 22.03.2022)

10 Flenov M. Ye. (2021) [Web-server glazami khakera – 3-ye izdaniye, pererabotano i dopolneno – SPb.: BKHV-Peterburg], Web server through the eyes of a hacker, 3rd edition, revised and updated.

11 Blog organizatsii IT GUILD, Kak SecOps prevrashchayetsya v instrument podderzhki lyubykh biznes-operatsiy. https://it-guild.com/info/blog/kak-secops-prevrashhaetsya-v-instrument-podderzhki-lyubyh-biznes-operaczij/(Data obrashcheniya 22.03.2022)

12 Aytkhozhayeva YU.ZH., Ziro A.A., Zhaybergenova Zh. A., Baltabay A.G. Testirovaniye na proniknoveniye. Vestnik Natsional'noy akademii nauk Respubliki Kazakhstan, №6 (376).- Almaty: Nauka, 2018. - S.39-44. ISSN: 1991-349421. DOI: 10.32014/2018.2518-1467.25. (Scopus, Web of Science, IF 0,094 po KazBTS).

13 Gnatyuk S. Critical Aviation Information Systems Cybersecurity? NATO Science for Peace and Security IOS Press Ebooks, 2016. Vol.47. – №3. – P. 308-316.

14 National Institute of Standards and Technology Special Publication 800-115 Natl. Inst. Stand. Technol. Spec. Publ. 800-115, 80 pages (Sep. 2008)

15 Goel S., Chen V. «Information security risk assessment – a matrix-based approach». University at Albany, SUNY. 2005.

16 Imran, M. S., &Mondal, S. A. (2013). The effect of marketing audit to enhance company performance and marketing accountability. Retrieved from http://www.wbiconpro.com/523-Imran.pdf. 73 Kamil VANA, L. C. (2014). The Marketing Audit as a Method of the Evaluation of the Marketing Plan. 132.

17 Kotler, P. (2002). Marketing Management, Chapter3: Winning Markets Through Strategic Planning, Implementation, and Control (Eleventh ed.). New Jersey, USA: Pearson Custom Publishing.